

Security Statement

Department: Operations

Version: 1.0

Last Update: 20.01.2009

Versions

No.	Date	Editor	Changes
1.0	Jan. 2009	SA2 Worldsync GmbH	Creation
Status:	final		

1 Introduction

1.1 Overview

This document outlines the security policies and procedures implemented by SA2 Worldsynchron to ensure that any sensitive data stored within an SA2 Worldsynchron application is protected from both external security risks and those internal to SA2 Worldsynchron.

These security topics are discussed from several perspectives:

- **Infrastructure & Network Security** - Network and infrastructure related security policies including:
 - Defense-in-depth: Multiple layers of protection and intrusion detection across the SA2 Worldsynchron network.
 - Well defined deployment and use of leading security technologies.
 - Highly robust, integrated and automated security functionality.
- **Application Security & Data Protection** – The measures taken at an application level to protect trading partner data include:
 - Internal security standards for internally developed products ensure that security standards are incorporated into our products at the code level.
 - Auditing of any external software (3rd party Off the Shelf software) for potential security risks.
 - Cryptographic Protocols for all communications over the public Internet (e.g. AS2, HTTPS, VPN, SSL, SSH etc) – Use of cryptography in securing communication channels, digital signatures, encrypting passwords in persistent storage.
 - Event analysis to ensure that any unauthorized access to customer data triggers an alarm and investigation.

1.2 Scope

This document provides an overview of the security measures implemented with SA2 Worldsynchron and does not provide a detailed listing of implementation specific aspects of security such as IP Addresses, ports, cryptographic protocols used and network architecture details.

More information regarding specific, non-sensitive aspects of the SA2 Worldsynchron security configuration including product specific features is available on request.

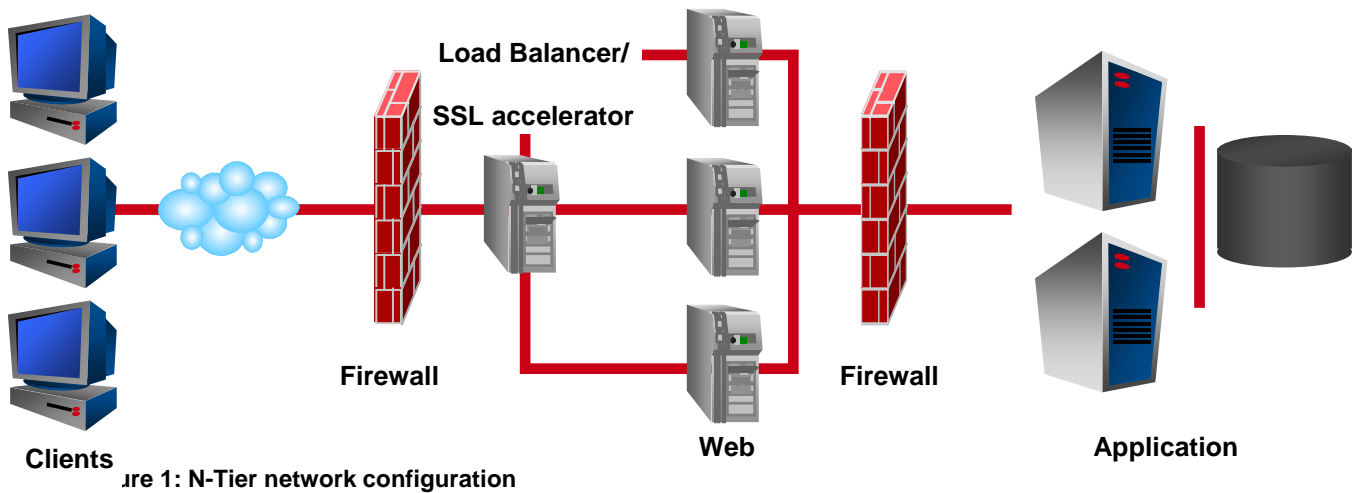


Figure 1: N-Tier network configuration

2.3 Bastion System Configuration

A bastion host is one that has been armored per the SA2 WorldsSync System Hardening requirements as part of the Defense-in-Depth strategy. These requirements include:

- Minimal operating system software – To prevent external Only those components of the operating system components that are required for the operation are installed.
- Minimal services running on each host – Only those services that are required for the system to function as expected are activated
- Network intrusion detection and alerting as described in Sections 2.4 below.
- Automated real-time monitoring of Network and application log.
- Cryptographic system integrity checking- Prevents unauthorized alteration of hard drive contents as described in Section 2.5 below.

2.4 Network Intrusion Detection

A number of network monitoring tools have been implemented to detect unwanted or malicious traffic:

- Signature-based IDS sensors:
 - Provides real time detection and alarming.
 - Network attacks can be recorded.
- Detection becomes more sensitive in proximity to information assets
- IDS sensors themselves are “stealth(ed)” and are not reachable from the Internet.

2.5 Host System Monitoring

In the event of unauthorized access to the SA2 Worldsinc network a number of system monitoring services have been implemented:

- Dedicated, isolated security monitoring, analysis and alarming services
- All events are centrally collected and analysed for suspicious events that may have occurred and potentially gone undetected by the real-time monitoring systems:
 - Network & firewall events
 - Operating system events
 - Database & application events
 - Intrusion detection & security alarms
- Additional near real-time event analysis allows for more complex, pattern-based intrusion identification.

2.6 Gateway Email Scanning

To prevent the entry of malicious third party applications all incoming and outgoing emails are scanned for viruses, worms, trojans, etc. Any infected email attachments are either cleaned or quarantined before being sent to their final destination

The SA2 Worldsinc anti-virus solution is deployed in a redundant configuration to ensure that the maximum protection is provided.

2.7 SA2 Worldsinc Business Premises Security

Access to the SA2 Worldsinc office locations is controlled by electronic badges.

3 Application & Data Security

In addition to the network and infrastructure level security, the SA2 Worldsinc suite of applications contain a number of security procedures designed to protect customer data.

3.1 Development Guidelines

In-house web-based applications are developed based on SA2 Worldsinc' secure development guidelines. These secure coding guidelines help SA2 Worldsinc build applications that are less likely to be vulnerable to attacks such as SQL Injection, XSS, etc.

Any security vulnerabilities that are identified are assigned a very high priority and fixed accordingly.

3.2 Application Access Management & Network Security

- All applications provide security features such as account intruder lock-out, password management and idle-session timeout.
- Applications implement role-based access control to restrict companies and users to their respective scope, both in terms of functionality and data access
- Applications are regularly tested for security vulnerabilities using a wide variety of web-application assessment tools
- Application/Web servers hosting the application are armored per SA2 Worldsinc security standards

3.3 System Security Event Analysis

The SA2 Worldsinc applications will track events and generate log entries and alarms based on the predefined severity levels. There are three levels of analysis of the security events tracked by the system:

- A single event occurs on one system (local atomic). For example: Someone trying to brute-force account passwords.
- Multiple events occur on one system (local composite). For example: Running exploits while scanning a given system.
- Cross-referenced events across multiple systems (complex composite). For example: Trying to run exploits while port-scanning the SA2 Worldsinc IP address space.

The event archives are stored in such a way as to allow for trend analysis and historical forensics as needed.

3.4 Communication Protocols

Communication between SA2 Worldsinc and its trading partners may use several communications channels:

- SA2 Worldsinc makes use of various cryptographic protocols to ensure confidentiality, integrity, authentication and non-repudiation.
- Our web-based applications support SSL/TLS for a 128-bit end-to-end secure connection between the client and the application
- AS2 is used as the primary protocol for machine-to-machine automated data transfer between SA2 Worldsinc and its partners
- Other communication mechanisms (browser or FTP client) utilize HTTPS (secure HTTP) and/or SFTP (Secure FTP)

3.5 System Hosting Physical Security

In addition to the application level security the SA2 Worldsinc systems are hosted in physically secure environments:

- The centers are generally located in state-of-the-art hosting facilities providing redundant power and communication links utilizing multiple power grids and service providers. For further details study the document "The PIRONET NDH Datacenter Home of the SA2 Worldsinc data pool".
- The data centers compliance with established standards and procedures is assured by an ITIL (IT Infrastructure Library)-compatible organizational structure for both services and processes, which forms an important foundation for our service-oriented outlook and actual provision of services.

3.6 Business Continuity Planning & Disaster Recovery

In the event that there is an interruption in service due to a hardware malfunction or other "disaster" SA2 Worldsinc will be able to recover the trading partner's data. Disaster recovery procedures include:

- SA2 Worldsinc hosts its applications in multiple data centers in geographically dispersed locations to provide business continuity in the event of a disaster
- Backup media is stored both onsite (in a fireproof safe) as well as offsite in a secure location as part of the Business Continuity (BC) and Disaster Recovery (DR) plan
- SA2 Worldsinc has dedicated environments for development, testing, staging and production systems. This ensures separation of duty and code-promotion to ensure that code deployed in production is free of backdoors, trojans, etc.